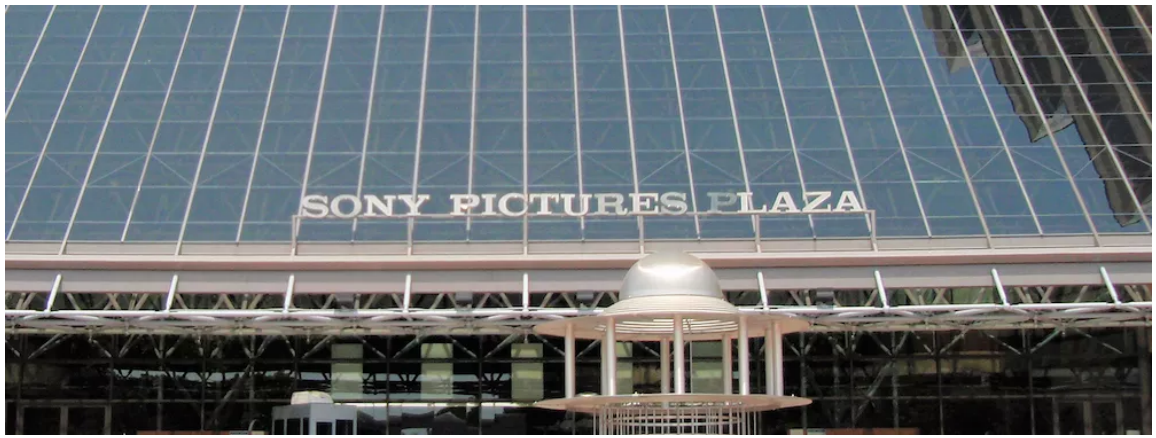
International Law and Cyber Attacks: Sony v. North Korea

By *Michael Schmitt*

Wednesday, December 17, 2014 at 9:29 AM



It could only happen in the movies. A major Hollywood company produces a film starring well-known comedic actors which involves the tongue-in-cheek assassination of the leader of a remote and rather bizarre dictatorship. The "supreme leader" apparently orders a secret group of cyber warriors calling themselves "The Guardians of Peace" (in actuality, the State-run "Bureau 121") to retaliate by attacking the company's IT system. Data is destroyed, sensitive personal data and highly embarrassing emails are made public and, worst of all, the script for the new James Bond movie is leaked. The international community is outraged, with some pundits calling it "war," while others claim that the operation has crossed the armed attack threshold thereby allowing the United States to respond forcefully. Send in the 7th Fleet….

But truth often proves stranger than fiction. With the exception of the U.S. Navy steaming towards North Korean shores, the description reflects recent events involving an alleged malicious North Korean cyber operation against Sony. This

contribution to *Just Security* analyzes the real world incident from an international law perspective. It draws on the work of the International Group of Experts (IGE) that produced the Tallinn Manual on the International Law Applicable to Cyber Warfare, as well as research underway in the "Tallinn 2.0" follow-up project.

Pursuant to Article 51 of the UN Charter and customary international law, if the malicious cyber operation against Sony had constituted a "use of force" rising to the level of an "armed attack," the United States would have been entitled to respond forcefully, whether by kinetic or cyber means. The IGE unanimously agreed that cyber operations alone may be sufficient to cross the armed attack threshold, particularly when they cause substantial injury or physical damage. Some members of the group went further by focusing not on the nature of the harm caused, but rather its severity. In their view, a sufficiently severe non-injurious or destructive cyber operation, such as that resulting in a State's economic collapse, can qualify as an armed attack.

The cyber operation against Sony involved the release of sensitive information and the destruction of data. In some cases, the loss of the data prevented the affected computers from rebooting properly. Albeit highly disruptive and costly, such effects are not at the level most experts would consider an armed attack. Additionally, some States and scholars reject the view that the right of self-defense extends to attacks by non-State actors. Even though the attribution of the Sony incident to North Korea has been questioned, this debate is irrelevant because the operation failed to qualify as an armed attack in the first place.

But was the operation nevertheless a violation of Article 2(4) of the UN Charter and customary international law's prohibition on the use of force by States such that it opened the door to responses other than forceful ones? The prevailing view in international law is that "use of force" is a lower threshold than "armed attack;" all armed attacks are uses of force, but the reverse is not true.

Unfortunately, after three years of discussion, the IGE could arrive at no black letter definition of a cyber use of force. Its members merely agreed that States would make case-by-case assessments of non-injurious or destructive cyber operations, considering such factors as severity, immediacy of effect, invasiveness, military character, and so forth.

Although the use of force threshold remains ambiguous, it seems highly unlikely that the international community will characterize operations like that against Sony as such. This hesitancy will be driven in part by concern over the U.S. position (a distinctly minority one) that all uses of force are also armed attacks that allow forceful responses. Some States view the premise as potentially destabilizing in that it allows for an earlier use of force than would otherwise be the case. They will accordingly be extremely reticent about characterizing cyber operations as having crossed that threshold.

Another possibility that can be dispensed with quickly is that the operation against Sony constituted an unlawful "intervention" against the United States. Disrupting a private company's activities is not the type of coercive action that intrudes into the domaine réservé of another State, thereby qualifying as intervention. Clear examples of intervention would include the financing of rebel forces examined by the International Court of Justice in its *Nicaragua* judgment, or even the election return manipulation cited by the IGE in its work—both well-removed from a cyber operation against Sony.

Much more defensible is characterization of the operation as a breach of U.S. sovereignty. To constitute a breach of sovereignty, an action must be attributable to a State. If North Korea's Bureau 21 mounted the cyber operation, there is no question of attribution since its hackers work for the military's General Bureau of Reconnaissance, and therefore are State "organs" whose actions are, as recognized in Article 4 of the ILC's Articles on State Responsibility, attributable to North Korea (even if acting *ultra vires*). If conducted by a non-State group, attribution for the operation would attach only if North Korea directed and controlled it (Article 8), or later acknowledged and adopted the action as its own (Article 11).

Assuming for the sake of analysis that the targeting of Sony is legally attributable to North Korea, the question remains as to whether it amounted to a breach of U.S. sovereignty. As an aside, it makes no difference that Sony is a private company, for the cyber infrastructure in question is situated in U.S. territory and therefore implicates U.S. sovereignty.

The substantive criteria for breach of sovereignty by cyber means has been the subject of extensive examination in the Tallinn 2.0 process. In the earlier *Tallinn Manual*, the IGE agreed that at the very least a cyber operation breached sovereignty whenever physical damage (as distinct from harm to data) occurred. While no further consensus could be achieved on the matter, it would seem

reasonable to characterize a cyber operation involving a State's manipulation of cyber infrastructure in another State's territory, or the emplacement of malware within systems located there, as a violation of the latter's sovereignty. This being so, if the cyber operation against Sony is attributable to North Korea, it violated U.S. sovereignty. In the patois of the law of State responsibility, the operation amounted to an "internationally wrongful act".

The commission of an internationally wrongful act entitles an injured State to engage in "countermeasures" under the law of State responsibility, as captured in Article 22 and 49-54 of the Articles on State Responsibility. Countermeasures are actions by an injured State that breach obligations owed to the "responsible" State (the one initially violating its legal obligations) in order to persuade the latter to return to a state of lawfulness. Thus, if the cyber operation against Sony is attributable to North Korea and breached U.S. sovereignty, the United States could have responded with countermeasures, such as a "hack back" against North Korean cyber assets. Indeed, it may still enjoy the right to conduct countermeasures, either because it is reasonable to conclude that the operation is but the first blow in a campaign consisting of multiple cyber operations or based on certain technical rules relating to reparations. It must be cautioned that the right to take countermeasures is subject to strict limitations dealing with such matters as notice, proportionality, and timing. Moreover, they are only available against States and the prevailing view is that a countermeasure may not rise to the level of a use of force.

If the operation is not attributable to North Korea as a matter of law, that State may nevertheless have been in breach of an obligation owed to the United States and other countries to ensure that cyber operations on its territory do not cause foreign States harm. Violation of this obligation of "due diligence" may itself provide a separate basis for countermeasures by injured States. In other words, if a territorial State fails to exercise due diligence in controlling non-State cyber operations launched from its territory, an injured State may resort to

countermeasures designed to compel that State to take the remedial measures to put an end to those activities. In the Sony case, even if the harmful cyber operation could not be attributed to North Korea under the law of State responsibility, the United States would have been entitled to conduct cyber operations against North Korea, or engage in other countermeasures, on the basis of North Korea's failure to discharge its due diligence responsibilities. Interestingly, countermeasures in such cases may consist of breaches of the territorial State's sovereignty in the form of hack-backs (below the use of force level) against the non-State actors operating from its territory. So, even though international law does not permit countermeasures against non-State actors on the basis of their own actions, operations against the non-State groups or individuals may be appropriate if styled as countermeasures against the States from which they act.

Countermeasures may only be taken by States. Thus, Sony could not have, on its own accord, responded against North Korea with its own cyber operations. That said, States are entitled to outsource the taking of lawful cyber actions to private entities; when they do so, the States shoulder legal responsibility for the actions.

A very limited, but highly important, basis for a State's response to harmful cyber operations is action pursuant to the plea of necessity, a notion reflected in Article 25 of the Articles of State Responsibility. In the cyber context, the rule applies only when harmful cyber operations affect the State's "essential interest" and the action is the only means to address "a grave and imminent peril" thereto. When this situation occurs, a State may take necessary actions that would otherwise be unlawful so long as the actions do not affect the essential interests of other States. There is no requirement in such situations that there be an initial "internationally wrongful act" or that, as in the case of countermeasures, the internationally wrongful act be attributable to a State. Thus, a plea of necessity is available in situations in which the author of a harmful cyber operation is either

a non-State actor or is unknown. It would appear indisputable that in the case of the operation against Sony, no essential U.S. interest was affected and therefore there was no legal basis to resort to the plea of necessity.

Completing the gamut of possible responses by States to harmful cyber operations mounted against them or entities on their territory is retorsion. Acts of retorsion are those that are unfriendly but lawful. For instance, barring any treaty obligation to the contrary, a State may close its cyber infrastructure to transmissions from another State in response to the latter's harmful cyber operations.

As this analysis illustrates, international law admits of a wide, although rather nuanced, range of possible response options in the face of malicious cyber operations. States and commentators would do well to recognize this reality. And, of course, all of the possibilities explored above are without prejudice to taking lawful measures under domestic law once jurisdiction attaches. Thus, for instance, those involved in the Sony incident risk prosecution under U.S. law in much the same way that five Chinese military hackers were indicted last May for computer hacking, economic espionage and other offenses.

The views expressed are those of the author in his personal capacity.

Tags: armed attack, Article 51, Cyber, Jus ad Bellum, Use of Force

ABOUT THE AUTHOR

Michael Schmitt is the Charles H. Stockton Professor of International Law and Director of the Stockton Center for the Study of International Law at the U.S. Naval War College. Follow him on Twitter (@Schmitt_ILaw).

SEND A LETTER TO THE EDITOR